REMARKS

This paper is responsive to a Final Office Action dated June 27, 2005. Prior to this response, claims 1-8, 10-25, and 27-35 were pending. After adding claim 36, claims 1-8, 10-25, and 27-36 remain pending.

Section 3 of the Office Action states that claims 1-8, 10-25, and 27-35 have been rejected under 35 U.S.C. 103(a) as unpatentable with respect to Mazzagatte et al. ("Mazzagatte"; US Patent 6,862,583), in view of DeBry (US Patent 6,385,728. With respect to claims 1, 12, 19, and 29, the Office Action states that Mazzagatte describes the claim elements of encrypting documents with a public key, spooling encrypted documents to a server, notifying the printer of spooled documents, accepting a private key at the printer, decrypting the documents using a private key, and printing. The Office Action acknowledges that Mazzagatte does not describe any public key encryption details, but states that DeBry describes using a symmetric key to encrypt documents, and encrypting the symmetric key with a public key. The Office Action states that it would have been obvious to combine Mazzagatte with DeBry because encrypting the document with a public key prior to transmission, where the private key is used for decryption, would prevent unauthorized printing and spoofing. This rejection is traversed as follows.

An invention is unpatentable if the differences between it and the prior art would have been obvious at the time of the invention. As stated in MPEP § 2143, there are three requirements to establish a *prima facie* case of obviousness.

> First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck* 947 F.2d 488, 20 USPQ2d, 1438 (Fed. Cir. 1991).

Generally, Mazzagatte describes a process that transmits an unencrypted document using a secure protocol, such as SSL, to a printer, along with a form of identification (Fig. 5). At the printer, the document is encrypted and stored. Figs. 6, 7A, and 7B describe the operations performed at a printer. To print a document, the user presents identification to the printer. Then, the printer decrypts the document and prints it. As acknowledged in the Office Action, Mazzagatte does not discuss using a public key to encrypt the print job.

DeBry's encryption process is summarized in col. 11, lines 1-15. DeBry initially encrypts a document, at the source, using a symmetric key. Then, the symmetric key is encrypted using the printer's public key. The Applicant notes that a symmetric key is not a public or private key, but rather, a secret key. The encrypted document and encrypted symmetric key are stored on a print server. At print time, the printer accepts the encrypted document and the encrypted symmetric key from the server. The printer uses its private key to decrypt the encrypted symmetric key. Then, it uses the symmetric key to decrypt the document.

With respect to the first *prima facie* requirement, the motivation to combine cannot be based upon a desired result of preventing "unauthorized printing and spoofing", as suggested in the Office Action.

Rather, the motivation must come a process detail of the DeBry system that can be applied to the Mazzagatte system. Further, even if an actual motive for combining references can be found, the combination of references does not suggest a modification to one (or both) of the references that makes the claimed invention obvious.

In fact, the combination of references suggests an invention that, unlike the claimed invention, can be spoofed. As noted above, Mazzagatte's system only encrypts a document at the destination printer. Mazzagatte's system provides very limited safeguards. In DeBry's system a spoofer can intercept documents if they are able to fake the certification of a system printer. Once the system accepts the public/private key of a spoofer as legitimate, the spoofer can intercept documents. The source encrypts its symmetric key using a public key that has been "verified". The flaw in the system is that the source sends its symmetric key along with the document. Since the symmetric key has been encrypted using a spoofer's public key, the spoofer is able to easily decrypt the symmetric key and gain access to the document.

The issue of motivation does not concern itself with whether there is some element of commonality between references. If it did, then any two references could be combined merely as the result of a common keyword. Although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion of motivation in the references to do so." *In re Mills*, 916 F.2d 680, 682, 16 USPQ2d 1430, 1432 (Fed. Cir. 1990). Here, the analysis must determine if there is any motivation to modify either Mazzagatte or DeBry in such a manner as to teach the claimed invention. DeBry may provide a

motivation to modify Mazzagatte, to perform some kind of encryption process. However, it is not the claimed invention process.

The proof of this statement can be seen in the operation of the claimed invention. In the claimed invention, the document is encrypted using a key pair where the user controls the private key, rather than accessing someone else's public key (associated a private key beyond the control of the user). Further, even if the document is misdirected or stolen in route to the printer, the document cannot be decrypted. In fact, even if the document is sent to the correct printer, the document cannot be stolen by someone who "runs to the printer" before the user, because the encryption cannot be enabled until the user arrives at the printer and enters their private key. Even if the prior art references are combined, they do not suggest the use of a private key as recited in the claimed invention, which prevents a document from printing until the user presents the private key.

Considered from the perspective of the second *prima facie* requirement, even if an expert were given the Mazzagatte and DeBry inventions as a foundation, there is no reasonable expectation that this expert could derive the claimed invention, since the claimed invention describes an invention where the user (the person printing a document) holds the private key.

With respect to the third *prima facie* requirement, even if the references are combined, they do not disclose all the elements of the claimed invention. The Applicant's base claims recite encrypting a document with a public key, accepting a private key at the printer, and decrypting the document with the private key. Mazzagatte does not describe the transmission of a document using a public/private key pair.

DeBry does not describe any of claimed invention steps either. Generally, DeBry describes a conventional digital envelope process. DeBry encrypts the document using a symmetric key, which is generally understood to be a randomly generated, secret key. When the randomly generated symmetric key is encrypted using a public key, a "digital envelope" is created. The symmetric key-encrypted document and digital envelope are transmitted together. The recipient's private key is used to recover the symmetric key from the digital envelope, so that the document can be encrypted. This process is explained in more detail in the Cryptology primer, Section 3.2 (page 3), which is enclosed as Attachment A.

In summary, neither of the prior art references describes a process that encrypts a document with a public key at the source, or decrypts the document at the destination printer using a private key. As mentioned above, the practical result of the Applicant's limitations is an added security enjoyed by neither of the references. Only the claimed invention limitations prevent a document from printing, until the user arrives at the printer and submits their private key.

The combination of Mazzagatte with DeBry does not explicitly describe all the limitations of claims 1, 12, 19, and 29. Neither do the references suggest any modifications that that make the Applicant's independent claims obvious. Claims 2-8 and 10-11, dependent from claim 1, claims 13-18, dependent from claim 12, claims 20-25 and 27-28, dependent from claim 19, and claims 30-35, dependent from claim 29, enjoy the same distinctions from the cited prior art, and the Applicant requests that the rejection be removed.

The affidavit of Joey Lum is enclosed as Attachment B, to support the Applicant's assertions. In summary, it is the opinion of Mr.

Lum that the prior art inventions permit the private key to be held by other entities than the user, because of different security concerns. Mazzagatte is primarily concerned with the security of the printer and DeBry is primarily concerned with the security of the file source. This difference in security focus teaches away from protecting the user, and granting the user access to the private key, as recited in the claimed invention.

Claim 36 is a new claim that has been added. Claim 36 is the same as the original claim 1, prior to claim 1 being amended. The combination of Mazzagatte and Debry does not disclose a process that encrypts a document with a public key at the source, or decrypts the document at the destination printer using a private key. Therefore, the limitation of "spooling the encrypted documents to a network-connected file server" is unnecessary to distinguish claim 36 from the prior art.

It is believed that the application is in condition for allowance and reconsideration is earnestly solicited.

Respectfully submitted,

Date: 8/18/2005

Gerald Maliszewski
Registration No. 38,054

Customer Number 55,286
P.O. Box 270829
San Diego, CA 92198-2829
Telephone: (858) 451-9950
Facsimile: (858) 451-9869
gerry@ipatentit.net